JPW
3621

**Edward Federowicz**
**98 West 32nd Street**
**Bayonne, New Jersey 07002**
**Phone 201.339.0502**
**E-mail lspma2@aol.com**

July 25, 2005

United States Patent & Trademark Office
Commissioner For Patents
Box 1450
Alexandria, VA 22313-1450

Re: Application No. 09/940.211 "SHIFT"

Dear Sir – Madam:

On December 10, 2004, I had a telephone communication with Examiner Christina Owen Sherr regarding an Office Action dated Nov. 17, 2004.. The a result of that communication, Ms. Sherr directed that I memorialize the content of the conversation in writing and mail it to her.. A copy of the four (4) pages sent to Ms. Sherr is attached.

Approximately three months later, I again called Ms. Sherr, at which time she told me that she ***did*** receive the Dec. 10th missive but said that the Patent Office did not receive the documents and that therefore they were not officially filed. When I requested that Ms. Sherr inform them that she received the documents, she responded that she was not able to do that and that I would have to write the Patent Office and explain the problem.

While in the process of formulating a letter to the Patent Office, while looking for earlier documents to attach, I took note that the response that I made to Ms. Sherr in regard to an Oct.19, 2004 Office Action, that it (the response) had the same exact address that the Dec. 10, 2004 response had, which Ms. Sherr received and acted on. At that point I again called Ms. Sherr and informed her that both documents had the same exact address, (including the attention to Ms. Sherr) and that she received and acted on the first, but that she did not react to the Dec. 10, 2004 response.. Once again Ms. Sherr said I would have to write the Patent Office.

At that point, I composed a letter (with attachments) and mailed it to the Patent Office. After again waiting a few months, and not receiving a response of any nature, I attempted to call Ms. Sherr and discovered that the phone number noted in the office Action (703-305-0625) was no longer in operation. Hence this communication.

Unfortunately, in the interim period my computer crashed and I lost all of the documents noted above.. However, Ms. Sherr may have a copy and if nothing else, can confirm my calls and concerns as noted above.

I timely responded to the Office Action of Nov. 17, 2004 and it was received by Ms. Sherr. I would like to know why no action was taken being that all responses' contained the same mailing address and was received by Examiner Sherr.

I would also appreciate if the patent application would be reinstated and processed and that I be informed of what action the Patent Office will take under the circumstances noted above.

Respectfully submitted,

Edward Federowicz

c: Cristina Owen Sherr (Examiner)
James Trammel (Supervisor)

# Memorandum Of Dec. 10, 2004 Telecom

As noted, this is the attempted clarification of the "Identity Theft" prevention component in Claim 6.

It is respectfully submitted that neither of the Ginter patents cited contain any component applicable to preventing identity theft.

In a nutshell, this invention serves to prevent Identity Theft by recording and digitizing the distinct voice patterns of an individual and storing the digitized voice pattern in a database. If anyone other than the "genuine" person would attempt to obtain credit under that name, the credit issuer, through "FICO" or other credit reporting agencies, is directed to the "VoiceGuard My ID" database and the person seeking credit is requested to speak their name. Being they are not the original party, their voiceprint will not match and they would be exposed as a person attempting to steal the identity of the original party. This person would then be taken into custody and the original party would be notified.

The "SHIFT' Claim 6, identity theft prevention component (operated as "VoiceGuard My ID") functions in the following manner:

## The "VoiceGuard My ID" Registration Process

A prospective Client would go to the "VoiceGuard My ID" web site and would be informed in detail of how the "VoiceGuard My ID" system operates to protect them from having their identity stolen.

If they elect to sign up, they would read directions on how they must fill out an enrollment form with basic personal information and pay for the "VotceGuard My ID" service with a personal Credit Card.

One of the following (or additional) processes would then be employed to verify that the prospective Client is the "genuine" person that they purport to be.

1 They would be required to supply the name/address of the bank and a number of one of their bank accounts at the bank they will be going to. The client would then receive an 800 number and a code number and would be instructed to go to their bank and to request that a bank officer assist them in registering their voice with "VoiceGuard My ID"

At the bank they then request a Bank official to call the "800" # and to provide the "code number". At that point, a "VoiceGuard My ID" representative asks the Bank Officer to confirm that the individual is the person they are asserting that they are. If the Identity is positively confirmed by the Bank Official, the person is given the phone and requested to say their name and address and a series of words or numerals (used as a PIN) and their Social Security number and to then repeat the same information a second time.

2. The prospective Client would go to the web site and enroll as described above. The Client would be provided with an 800 and a "code number" and would be instructed to fax or mail a copy of a picture driver's license to that number. They would also be informed that a "VoiceGuard My ID" representative would call their home phone at a random time so as to confirm that they are the person on the picture driver's license.

The "VoiceGuard My ID" representative would record and digitize the Client's voice and store it in the "VoiceGuard My ID" database.

An existing "voice digitization" system is to be licensed and employed to digitize the name, address, PIN and Social Security number of the Client and the digitized sample is then entered into a secure "VoiceGuard My ID" database.

# The "VoiceGuard My ID" Identity Protection Process

The Client's digitized voice sample is then "flagged" in the databases of "Fico" (Fair-Isaacs) and similar type credit databases. Whenever anyone attempts to obtain any form of new credit under that name, the "flag" in the credit information system's databases direct the request to the "VoiceGuard My ID" database.

The "VoiceGuard My ID" database then provides a. "different code number" and "800 Number" and directs that the Credit Issuer have the person call the 800 number and when requested for the "code number" to enter it, at which time the "VoiceGuard My ID" database system searches for that specific "code number" from winch it takes a "COPY" of the genuine registered Client's digitized voice and places it in a separate disposable "module".

That "module" then requests the credit applicant to say their name, address, Social Security number and PIN, which is then instantly digitize and compared to the "genuine" voiceprint of the "genuine" person contained in the "module". If the digitized voices match, then "VoiceGuard My ID" informs the Credit Issuer that the credit applicant is the person they purport to be and that credit may be given if ail else warrants.

If the digitized voice does not match the voice of record, then the Credit Issuer is informed that an "Identity Theft" is being attempted and to detain the party and to call their security personnel or the police.

The "VoiceGuard My ID" system then contacts the registered Client and informs them of the attempt and provides them with the phone number of the Credit Issuer and recommends the registered Client determine if they know the person who attempted to steal their Identity in order to give the registered Client the final say of if they want the person prosecuted, this in the event that it was a family member that they may not want prosecuted. This information of attempted Identity tliefts are then stored in a separate and different database for security reasons.

# The "VoiceGuard My ID" Module

The "VoiceGuard My ID" database is kept secure at all times. There is no direct Internet access to the prime "VoiceGuard My ID" database. Hence the prime database can never be available to Hackers.

When a verification request comes to an Internet access "VoiceGuard My ID" computer, that computer, after going through a number of "firewalls" employs the "code number" to request a "COPY" of the particular Client's sample voice, which is placed in a special "module" that also contains a voice digitization mechanism, which is then used for the voiceprint verification process as described above.

Once the "module" completes a comparison process, the results are then sent back to a second and totally separate "VoiceGuard My I.D" database that is accessible only by the name of the Client, the social security number and PIN first being deleted. Once this process is complete, the "module" self destructs.

This faction of the "VoiceGuard My ID" process is specifically designed and intended to prevent unauthorized persons from obtaining any form of "NEW" credit under a registered Client's name.

# Optional Credit Card Security Faction

A second available process of "VoiceGuard My ID" is designed to protect the theft and misuse of credit cards.

With this process, a Client would determine a purchase limit for their credit cards and/or a specific number of high priced purchases that could be made with their card within a twelve (12) hour period. If the Client selects a Two Hundred ($200.00) Dollar (or any given amount) limit on any credit card purchase, that specific amount would be registered, by virtue of a "flag" on the persons name at their credit card issuer database.

In the event the card was stolen or was being misused for purchases over the specified amount, the credit card issuer database "flag" would contact the "VoiceGuard My ID" database and the voiceprint verification process described above would he employed to verity whether or not the party was the "genuine" person entitled to use the card.

This faction of "VoiceGuard My ID" would serve to prevent any extreme loss if a credit card was stolen or misused.